keep a record of the vaults and security containers under their cognizance along with the designation of the level of classified information authorized to be stored therein.

§ 17.76 Changing combinations to security containers.

Combinations to security containers and dial-type locks will be changed only by individuals having an appropriate security clearance and who have received instruction on how to correctly change such combinations. Combinations shall be changed:

(a) When the container is placed in use;

(b) When an individual knowing the combination no longer requires or is authorized access to classified information stored in the container;

(c) When the combination or record of combination has been subject to compromise;

(d) When taken out of service; or

(e) At least annually.

§ 17.77 Equipment out of service.

When security storage equipment is taken out of service, it shall be inspected to ensure that no classified information remains.

(a) Security Programs Managers shall establish procedures to certify that whenever security equipment is moved or relocated or ''out of service'' or ''excess'' that the security equipment does not contain classified information.

(b) When taken out of service, built-in combination locks shall be reset to the standard combination 50–25–50. Combination padlocks shall be reset to the standard combination 10–20–30.

§ 17.78 Classification of combinations.

The combination of a vault or container used for the storage of classified information and material shall be assigned a security classification no lower than the highest level of the classified material authorized to be stored therein. No downgrading/declassification instructions or classifier identity are required to be made when classifying records of combinations to security containers. Accordingly, classification actions for such combinations are not required to be reported. Knowledge of combinations shall be limited to the minimum number of persons necessary for operating purposes.

§ 17.79 Recording storage facility data.

A record shall be maintained by Security Programs Managers or their designees for each vault, secure area, or container used for the storage of classified information. The record shall show its location, and the names and other appropriate identifying data of persons having knowledge of the combinations to such storage facilities. General Services Administration Optional Form 63, entitled, ''Security Container Information'' may be used within the Department for these purposes. The OF–63 containing security combinations shall be marked with the appropriate overall classification, and shall be safeguarded and stored in accordance with the protection afforded to that classification.

§ 17.80 Care during working hours.

Each individual shall take all necessary precautions to prevent access to classified information by unauthorized persons (i.e., persons who do not possess an appropriate security clearance, and who do not possess the required need-to-know). Among the precautions to be followed are:

(a) Classified documents, when removed from storage for working purposes, shall be kept under constant surveillance and turned face-down or covered when not in use. Department Cover Sheets should be utilized to cover classified documents.

(b) Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information shall be either destroyed by the person responsible for their preparation immediately after they have served their purposes, or shall be given the same classification and safeguarded in the same manner as the classified information they contain.

(c) Classified information handled by word processors or remote terminals is susceptible to interception by unauthorized persons due to unintended electrical emanations. Word processors or remote terminals used frequently to handle classified information must

have a reduced level of emanations (e.g., approved by the Subcommittee on Compromising Emanations) or located in an area with a sufficient perimeter of control.

(d) Typewriter ribbons used in typing classified information shall be protected in the same manner as the highest level of classification for which they have been so used. When destruction is necessary, it shall be accomplished in the manner prescribed for classified working papers (See subpart H) of the same classification. After the upper and lower sections of the ribbon have been cycled through the typewriter five times in the course of regular typing, all fabric ribbons may be treated as unclassified. Carbon and plastic typewriter ribbons and carbon paper which have been used in the production of classified information shall be destroyed after initial usage in the manner prescribed for working papers of the same classification. As an exception to the foregoing, any typewriter ribbon which remains substantially stationary in the typewriter after it has received at least five consecutive impressions may be treated as unclassified.

§ 17.81 Care after working hours.

Heads of Offices, Boards, Divisions and Bureaus shall require and institute through their Security Programs Managers, a system of security checks at the close of each working day to ensure that the classified information in the possession of such Offices, Boards, Divisions and Bureaus is properly protected. Security Programs Managers shall require the custodians of classified information in their Offices, Boards, Divisions or Bureaus to make periodic inspections of their respective areas which shall ensure that the following minimum requirements are met:

(a) All classified information is stored in approved security containers. This includes removable storage media, e.g., floppy disks used by word processors, that contain classified information.

(b) Burn bags, if utilized, are either stored in approved security containers or destroyed.

(c) Classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts and similar papers have been properly stored or destroyed.

§ 17.82 Administrative aids for safeguarding classified material.

Appropriate forms shall be used on security containers for check purposes. Such forms shall be conspicuously attached to the outside of each container used for the storage of classified information. Each authorized person will record the time and date that he or she unlocks or locks the security container, followed by the person's initials. At the close of each working day, a person other than the individual locking the container will check the container, in the presence of the individual locking the container, to ensure that it is secure. The time of the check followed by the checker's initials will be recorded. The check will be conducted each working day. If a container has not been opened, the date and the phrase ''Not Opened'' will be noted in addition to the time and the checker's initials. A container will not be left unattended until it has been locked by an authorized person and checked by a second person. The person locking a container is responsible for insuring that another person checks the container. Reversible ''OPEN-CLOSED'' signs, shall be utilized on security containers containing classified information. The respective side of the sign shall be displayed to indicate when the container is open or closed.

§ 17.83 Telephone or telecommunication conversations.

(a) Classified information shall not be discussed over nonsecure telephones. Classified telephone conversations are authorized only over approved secure (encrypted) communication circuits. Information concerning which telephones in the Department are secure may be obtained from Security Programs Managers or the Department Security Officer.

(b) Classified information shall not be transmitted over nonsecure radio equipment or facsimile devices. Classified information may be transmitted